

**RON WYDEN**  
OREGON

221 DIRKSEN SENATE OFFICE BUILDING  
WASHINGTON, DC 20510  
(202) 224-5244  
(202) 224-1280 (TDD)

**United States Senate**  
WASHINGTON, DC 20510-3703

**COMMITTEES:**

COMMITTEE ON THE BUDGET

COMMITTEE ON ENERGY AND NATURAL RESOURCES

SUBCOMMITTEE ON PUBLIC LANDS AND FORESTS

SPECIAL COMMITTEE ON AGING

SELECT COMMITTEE ON INTELLIGENCE

COMMITTEE ON FINANCE

August 8, 2019

Michel Combes  
Chief Executive Officer and President  
Sprint Corp.  
6200 Sprint Parkway  
Overland Park, KS 66251

Randall L. Stephenson  
Chairman and Chief Executive Officer  
AT&T Inc.  
208 South Akard Street  
Dallas, TX 75202

John Legere  
Chief Executive Officer  
T-Mobile US, Inc.  
12920 Southeast 38th Street  
Bellevue, WA 98006

Hans Vestberg  
Chief Executive Officer  
Verizon Communications Inc.  
1095 Avenue of the Americas  
New York, NY 10013

Dear Mr. Combes, Mr. Legere, Mr. Stephenson and Mr. Vestberg:

I write to ask that you protect your customers' privacy — and U.S. national security — from foreign hackers and spies by limiting the time you keep records about your customers' communications, web browsing, app usage and movements.

In recent years, the U.S. Office of Personnel Management (OPM), the health care company Anthem, and the hotel chain Starwood have all been hacked. In addition to impacting the privacy of millions of Americans whose information was stolen, these breaches also threaten U.S. national security. Personal data can be used by foreign intelligence services to support their espionage and influence operations. In 2015, then-Director of National Intelligence James Clapper said that China was the "leading suspect" in the theft of data from OPM.

Your companies collectively hold deeply-sensitive information about hundreds of millions of Americans. It should come as no surprise that this data is a juicy target for foreign spies. Particularly in this modern era of massive data breaches, it is critical that companies like yours minimize the data you keep. As the Federal Trade Commission (FTC) noted in a 2015 report, "Thieves cannot steal data that has been deleted after serving its purpose; nor can thieves steal data that was not collected in the first place."

While the Federal Communications Commission (FCC) has long required carriers to keep records of toll calls for 18 months, it is apparently routine for carriers to retain records for much longer. According to media reports, for example, AT&T retains customer long distance and international call records going back to 1987. This data hoarding by telephone companies is unnecessary — firms do not need 20 years' worth of customer records to manage their networks — and these stockpiles of Americans' data create an irresistible target for hackers and foreign governments.

911 NE 11TH AVENUE  
SUITE 630  
PORTLAND, OR 97232  
(503) 326-7525

405 EAST 8TH AVE  
SUITE 2020  
EUGENE, OR 97401  
(541) 431-0229

SAC ANNEX BUILDING  
105 FIR ST  
SUITE 201  
LA GRANDE, OR 97850  
(541) 962-7691

U.S. COURTHOUSE  
310 WEST 6TH ST  
ROOM 118  
MEDFORD, OR 97501  
(541) 858-5122

THE JAMISON BUILDING  
131 NW HAWTHORNE AVE  
SUITE 107  
BEND, OR 97701  
(541) 330-9142

707 13TH ST, SE  
SUITE 285  
SALEM, OR 97301  
(503) 589-4555

Accordingly, I urge you to take prompt action to protect your customers' privacy and safety, as well as U.S. national security, by significantly limiting your retention of customer data. Consistent with the best practices recommended by the FTC and leading privacy experts, absent a legal requirement to retain specific records, you should delete records of your customers' historical location, their web browsing, app usage and their communications as soon as those records are no longer needed to reasonably manage your networks and provide service. Depending on the specific type of record and the legitimate business purpose they serve, a reasonable retention period could be a few weeks, or even just a couple days. Retention periods of several years should not be the norm.

Please respond to this letter by September 4, 2019 detailing the steps you will take to protect your customers' privacy and U.S. national security by minimizing your retention of customer data.

Thank you for your prompt attention to this important matter. If you have any questions about this request, please contact Chris Soghoian in my office.

Sincerely,



Ron Wyden  
United States Senator